April
2017

EMEA
EDITION

netskope

CLOUD REPORT

MORE THAN HALF OF MICROSOFT OFFICE 365 USAGE COMPRISED OF SERVICES OTHER THAN ONEDRIVE FOR BUSINESS

REPORT HIGHLIGHTS

- 56.75 per cent of Microsoft Office 365 usage comes from services other than OneDrive for Business.
- Enterprises have an average of 903 cloud services in use, up from 845 of last quarter.
- Microsoft again dominates list of top 20 cloud services used, with 8 total services on the list.
- Backdoors make up the majority of cloud malware detections at 37.1 per cent, with ransomware at 4.2 per cent.

EXECUTIVE SUMMARY

In this Netskope Cloud Report™, we've compiled the most interesting trends on cloud service adoption and usage based on aggregated, anonymised data from the Netskope Active Platform™. Report findings are based on usage seen across millions of users in hundreds of accounts globally and represent usage trends from October 1 through December 31, 2016.

This quarter, we did an analysis of Microsoft Office 365 usage and found that 56.75 per cent of usage comes from services other than OneDrive for Business. This means that security professionals should not only focus on OneDrive, but also gain visibility and control over other apps and services like SharePoint, Dynamics, Power BI, Teams, Outlook.com, and others (including ecosystem services) for full protection of sensitive data and risky activities. Security teams will need ensure they are able to see the activity and place access, security, and DLP controls on these other services.

Up around 7 per cent (from 845 last quarter), this quarter's average number of cloud services in use by enterprises is 903. Microsoft took 8 spots on the list of top 20 used cloud services, with services like OneDrive, Outlook, and SharePoint. Fast becoming the de facto platform of choice for organisations, we continue to see Microsoft's reach in our top 20 list. Slack and ServiceNow appeared on the list in the past two quarters and remain on it, at 15 and 18, respectively.

Send, create, and edit were the top cloud activities this quarter. In cloud storage services, view, edit, and download were the top activities, respectively, with share following download as a close fourth. The other categories of services had similar top activities as well, a good reminder for organisations to place activity-level controls on these services to restrict risky activities and protect sensitive data being shared.

For DLP violations this quarter, webmail edged out cloud storage services slightly to be the top category for DLP violations, with 39.9 per cent versus 39.0 per cent. The "other" category made up the rest with 21.1 per cent. By activity, upload led with 48.5 per cent, followed by send with 25.2 per cent download with 24.4 per cent, and other with 1.9 per cent. PII violations made up the majority this quarter in terms of type at 39.2 per cent. PHI followed at 24.8 per cent, source code 17.2 per cent, PCI 3.6 per cent, and all others 15.2 per cent.

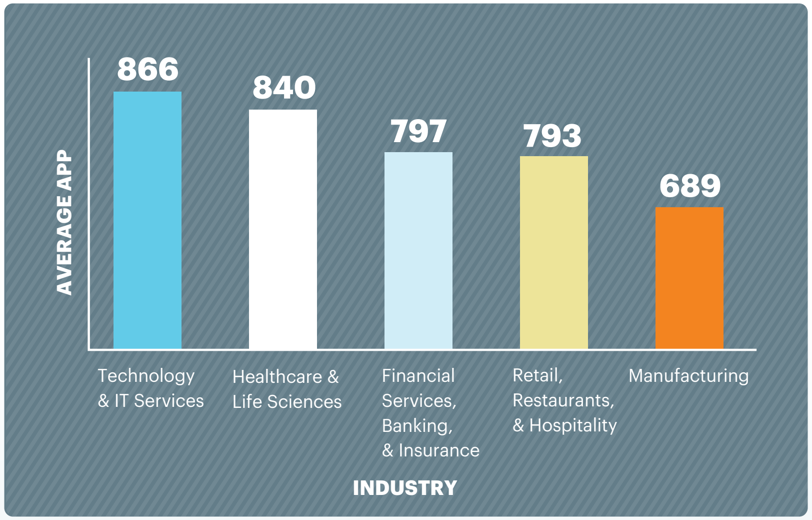
In this report we have also updated the malware findings from Netskope Threat Research Labs. This quarter, the category percentages are: 37.1 per cent of detections were backdoors, adware 14.3 per cent, Mac 7.4 per cent, Microsoft Office macros 6.0 per cent, Javascript malware 5.8 per cent, ransomware 4.2 per cent, mobile malware 1.5 per cent, PDF exploits 1.0 per cent, and all others 22.7 per cent. The percentage of malware-infected files shared with others, including internal or external users, or publicly, continues to drop, from 26.5 per cent last quarter to 9.3 per cent this quarter. This may still be attributable to the fact that Netskope customers are increasingly using Netskope Threat Protection. In severity, high severity made up the most of the detections with 75.4 per cent, with low at 24.6 per cent.

ENTERPRISES USE AVERAGE OF 903 CLOUD SERVICES

This quarter, the average amount of cloud services per enterprise increased around 7 per cent to 903 cloud services, compared to 845 last quarter. 93.9 per cent of these services are not enterprise-ready, earning a rating of "medium" or below in the Netskope Cloud Confidence IndexTM (CCI).

The technology and IT services industry had the highest average amount of cloud services used at 866. Following that was healthcare and life sciences with 840, financial services, banking and insurance with 797, and retail, restaurant, and hospitality and manufacturing with 793 and 689, respectively.

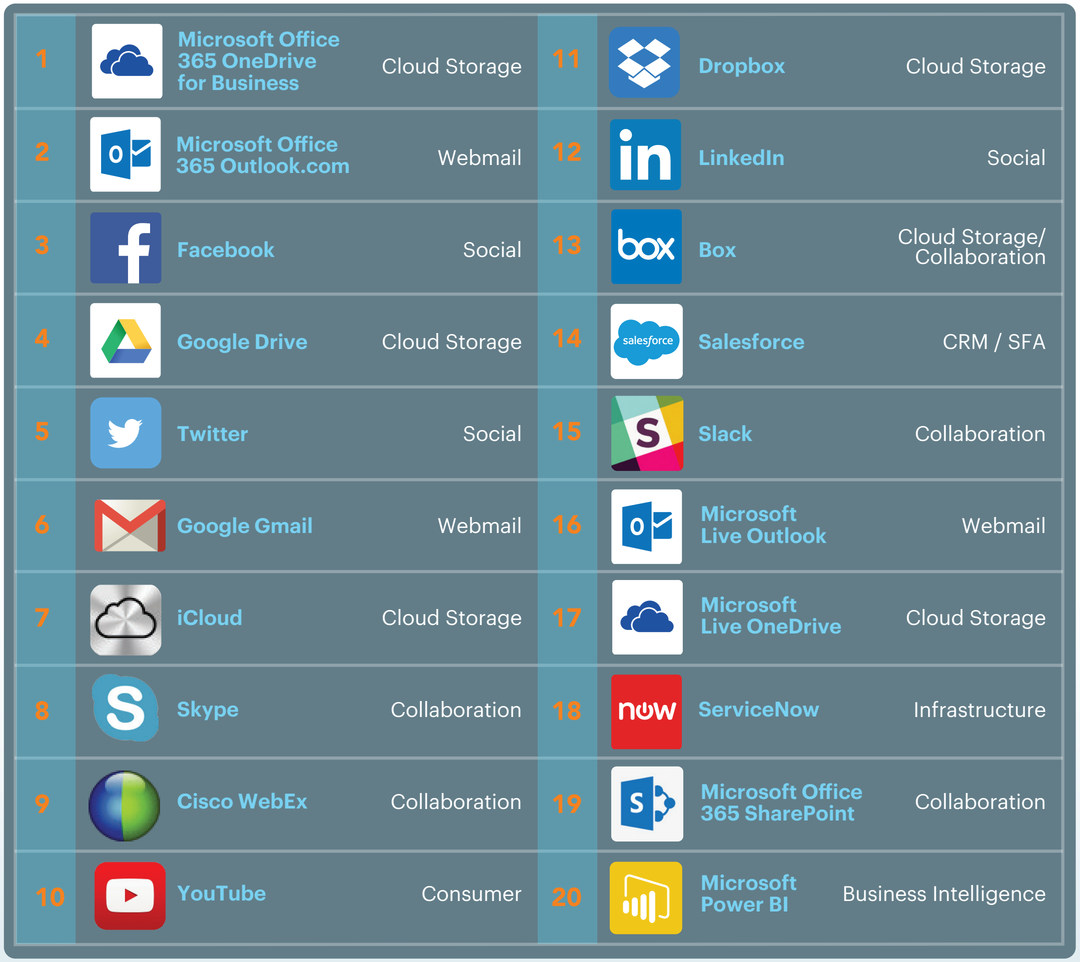
On the category side, marketing services led with an average of 81, followed closely by HR at 72. And as with previous quarters, the percentage that are not enterprise-ready have held steady at the respective numbers. With the rise of cloud malware and hackers compromising organisations via cloud services, it's critical to apply granular controls and inspect traffic from all locations (whether on-premises or off), devices, and apps (sync clients and native mobile apps included) for threats.



CATEGORY	# PER ENTERPRISE	% NOT ENTERPRISE-READY
Marketing	81	97%
HR	72	95%
Collaboration	68	88%
Finance/Accounting	57	96%
CRM/SFA	45	94%
Software Development	44	96%
Social	35	92%
Productivity	31	94%
Cloud Storage	29	76%
IT Service/Application Management	26	98%

MICROSOFT LANDS 8 CLOUD SERVICES IN TOP 20 LIST

Microsoft takes the top two places in our top 20 cloud services list this quarter again. Office 365 is quickly becoming a platform for Microsoft – with services constantly being added and updated as well as partners integrating with their own external services and apps. A total of eight cloud services from Microsoft are on our list this quarter, including OneDrive for Business, Office 365 Outlook.com, Skype, LinkedIn, and more. With the ever-increasing usage of Office 365 platform services at organisations, security professionals should remember that visibility and control should go beyond just OneDrive and SharePoint but also extend that over services like Dynamics, Power BI, Teams, and more, as well as to ecosystem cloud services that connect to the Office 365 suite. Delve into the details of this in the next section of the Cloud Report, "Microsoft Office 365: Beyond OneDrive for Business."

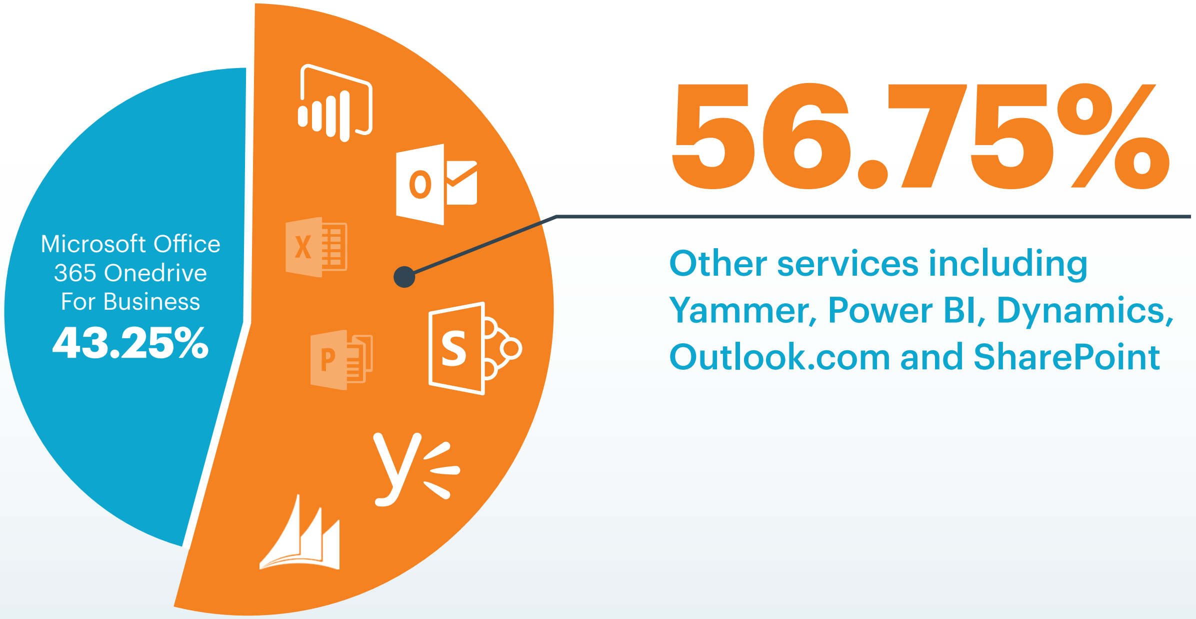


1	Microsoft Office 365 OneDrive for Business	Cloud Storage	11	Dropbox	Cloud Storage
2	Microsoft Office 365 Outlook.com	Webmail	12	LinkedIn	Social
3	Facebook	Social	13	Box	Cloud Storage/ Collaboration
4	Google Drive	Cloud Storage	14	Salesforce	CRM / SFA
5	Twitter	Social	15	Slack	Collaboration
6	Google Gmail	Webmail	16	Microsoft Live Outlook	Webmail
7	iCloud	Cloud Storage	17	Microsoft Live OneDrive	Cloud Storage
8	Skype	Collaboration	18	ServiceNow	Infrastructure
9	Cisco WebEx	Collaboration	19	Microsoft Office 365 SharePoint	Collaboration
10	YouTube	Consumer	20	Microsoft Power BI	Business Intelligence

MICROSOFT OFFICE 365: BEYOND ONEDRIVE FOR BUSINESS

Looking into the usage of Microsoft Office 365 across all Netskope customers, we've found that a full 56.75 per cent of Microsoft Office 365 usage is comprised of services other than OneDrive for Business. These services include Yammer, Power BI (which made the top 20 list this quarter), Dynamics, Outlook.com, SharePoint, and more. This stat is a good reminder that OneDrive is not the only cloud service that needs to be secured in Office 365. Sensitive data can also be uploaded to and shared and sent from services like Power BI (share is the top activity in business intelligence services, as indicated by the next section of the report), a business intelligence tool by Microsoft or Dynamics, a CRM tool. We recommend security professionals analyze what Office 365 services (other than OneDrive for Business) are in use across their organisation and place appropriate access and security controls over these services (and also connected ecosystem services) for comprehensive protection.

MICROSOFT OFFICE 365 USAGE



TOP CLOUD ACTIVITIES

The top cloud activities this quarter were send, create, edit, login, view, download, invite, share, upload, and delete, respectively. Netskope normalises more than 50 possible cloud activities across cloud services within categories and even across categories, so whether a user shares a file from a cloud storage service or a report from a business intelligence one, each of those are recognised as a share activity. This is useful in understanding risk, auditing user activity, and being able to say deterministically whether a data policy violation has occurred. It is also useful in isolating policy enforcement to a risky activity like share, rather than only being able to allow or block a cloud service. Examining cloud service activities in the context of the category, we call out the top three activities besides login for each of five important business categories, cloud storage, HR, business intelligence, finance, and collaboration.

Top Activities in Cloud Storage

1. View
2. Edit
3. Download

Top Activities in HR

1. Create
2. Edit
3. Download

Top Activities in Business Intelligence

1. Share
2. View
3. Download

Top Activities in Finance

1. Edit
2. Download
3. Create

Top Activities in Collaboration

1. Edit
2. Create
3. View

TOP POLICY VIOLATIONS IN THE NETSKOPE ACTIVE PLATFORM

Beyond measuring usage and activity, we also look at policy violations within cloud services. Policies can be enforced based on a number of factors, including user, group, location, device, browser, cloud service, instance, category, enterprise-readiness score, DLP profile, activity, and more. Through data abstraction and normalisation of those factors, we're able to discern the services, categories, and activities surrounding a violation. Policies observed include blocking the download of PII from an HR service to a mobile device, alerting when users share documents in cloud storage services with someone outside of the company, and blocking unauthorised users from modifying financial fields in finance cloud services.

Here are the top activities globally that constituted a policy violation per cloud service category, with DLP violations noted where they apply. Just as activities can vary between services, policy violations involving those activities can vary. For example, a policy violation involving downloading from a cloud storage service can be the improper downloading of a non-public press release, whereas in a CRM/SFA service could signal theft of customer data by a departing employee.

Cloud service category	Delete	Download	Edit	Log In	Post	Send	Share	Upload	View
Cloud storage	7	3 !	2 !	6	8	–	4	5 !	1
Collaboration	3	4 !	1	7	5 !	9	8	6 !	2
Customer Relationship Management	8	5 !	3	2	6 !	9	1	7 !	4
Finance/ Accounting	3	5	2	1	–	–	7	6	4
HR	3	5	4	1	–	–	7	6	2
Productivity	1	5 !	4	2	–	–	3	7 !	6
Social	4	7 !	5 !	2	3 !	–	8	6 !	1
Software Development	6	3	1	4	8	–	7	5 !	2
Webmail	6	4 !	2	7	–	1 !	8	5 !	3

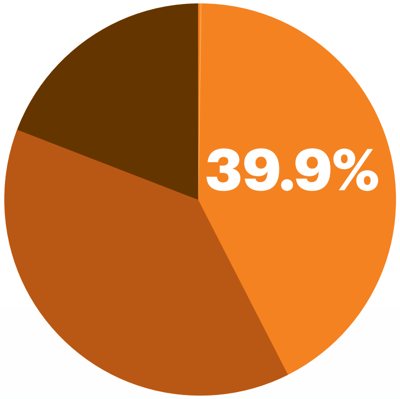
! Policy violation included in data loss prevention profile

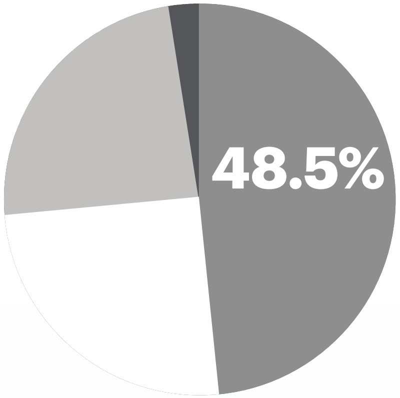
1 Indicates highest occurrence of policy-violating activity for the category

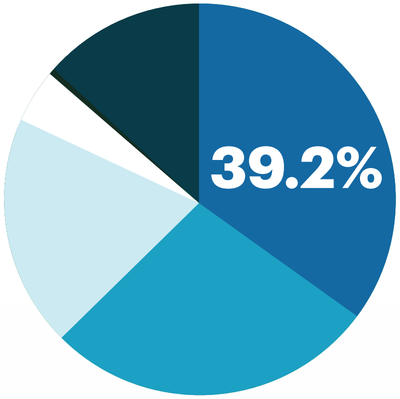
CLOUD DLP POLICY VIOLATIONS

In DLP violations by cloud service category this quarter, webmail pulled ahead of cloud storage with 39.9 per cent of all violations, cloud storage had 39.0 per cent, and everything else comprised 21.1 per cent. This may signal a maturity in Netskope customers as they are starting to focus on categories other than cloud storage. An example of this would be with Slack, a collaboration service, and how popular it is with organisations large and small. As companies build out their DLP programs and policies, they'll need to focus on services beyond cloud storage, like collaboration or business intelligence, depending on employee usage. DLP violations by activity stayed similar to last quarter, with uploads leading with 48.5 per cent, followed by send with 25.2 per cent, download 24.4 per cent, and other (including view) 1.9 per cent.

For file type violations, PII came in first at 39.2 per cent, followed by PHI with 24.8 per cent, source code 17.2 per cent, PCI 3.6 per cent, and all others 15.2 per cent. Anecdotally, we are seeing some usage of the Netskope EU GDPR DLP profile template, indicating some organisations are getting a headstart in GDPR compliance.







CATEGORY

- Webmail **39.9%**
- Cloud Storage **39.0%**
- Other **21.1%**

ACTIVITY

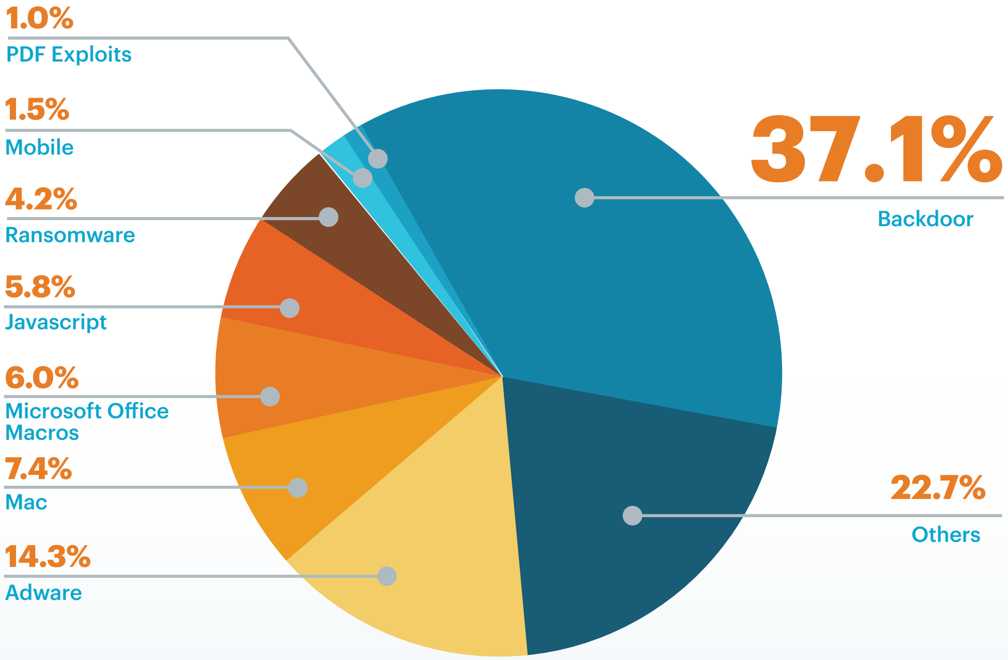
- Upload **48.5%**
- Send **25.2%**
- Download **24.4%**
- Other (including View) **1.9%**

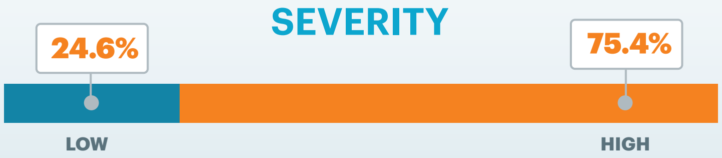
TYPE

- PII **39.2%**
- PHI **24.8%**
- Source Code **17.2%**
- PCI **3.6%**
- Other (including Confidential and Profanity) **15.2%**

CLOUD THREATS EVOLVE IN TYPE AND SEVERITY

Data from the Netskope Threat Research Labs for this quarter shows that backdoors made up the bulk of the detections at 37.1 per cent, a slight decrease from last quarter's 43.2 per cent. Following backdoors, adware was at 14.3 per cent, Mac malware at 7.4 per cent, and Microsoft Office macros at 6.0 per cent. Javascript took 5.8 per cent, ransomware 4.2 per cent, mobile 1.5 per cent, PDF exploits 1.0 per cent, and finally all others 22.7 per cent. The variability in detection types continue (possibly attributable to evolving and new threat types being created), but certain metrics have improved, like the fact that 9.3 per cent of malware-infected files were shared, compared to 26.5 per cent last quarter. This may be because of customers deploying Netskope Threat Protection and continually monitoring and setting up policies to guard against cloud threats. In severity, high severity made up the most of the detections with 75.4 per cent, followed by low at 24.6 per cent.





THREE QUICK WINS FOR ENTERPRISE IT

1 Ensure visibility and control across all Microsoft Office 365 services and connected ecosystem services, not just OneDrive for Business.

2 Place granular, activity-level controls over unsanctioned cloud services to defend against ever-evolving types of cloud threats and malware.

3 Complement DLP programs by using compliance regimen-specific templates and profiles to fulfill requirements from regulations like GDPR.